RFC-0018 FedRAMP Security Inbox Requirements

RFC Front Matter

- **Status:** Open
- **Created By:** FedRAMP
- **Start Date:** 2025-09-29
- **Closing Date:** 2025-10-29
- **Short Name:** rfc-0018-fedramp-security-inbox

Where to Comment

Members of the public may submit multiple different comments on different issues during the public comment period. The public is asked to please refrain from including documents or spreadsheets (especially those with in-line comments or suggested changes) in public comment as this creates a significant additional review burden.

Formal public comment for official consideration by FedRAMP can be made via the following mechanisms in order of preference:

1. GitHub Post: https://github.com/FedRAMP/community/discussions/92
2. Public Comment Form: https://forms.gle/JkQ7oQtTZPUSjztVA
3. Email: pete@fedramp.gov with the subject "**RFC-0018 Feedback**"

Note: FedRAMP will review and publicly post all public comments received via email, but will not otherwise respond. Email submissions from federal agencies will only be made public when requested by the agency.

Summary & Motivation

FedRAMP recently sent an emergency notification to the security contact addresses for all cloud service providers as part of the government-wide response to CISA's Emergency Directive 25-03 and discovered a systemic problem within the FedRAMP marketplace: a significant number of FedRAMP Authorized cloud services have failed to maintain their security contact information, have gated contact behind customer portals with required registration, or have otherwise cut themselves off from direct emergency communication from FedRAMP.

This proposed standard outlines clear requirements for cloud service providers to maintain a path for open communication from FedRAMP and government customers, especially during an emergency. It also explicitly outlines the punitive actions FedRAMP will take in the future against providers who do block critical communications and plans for FedRAMP to regularly assess the effectiveness of all provider's ability to receive communications from FedRAMP.

Once formalized, providers will have a limited time to adopt this policy and should expect an initial FedRAMP-wide assessment of compliance by the end of FY26 Q2.

Effective Date(s) & Overall Applicability

This is a draft standard released for public comment; it does not apply to any FedRAMP authorization and MUST NOT be used in draft form.

- FedRAMP **20x**:
    - This standard will immediately apply to all FedRAMP 20x authorizations when formalized.
- FedRAMP **Rev5**:
    - This standard will immediately apply to all FedRAMP Rev5 authorizations when formalized.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

OMB Memorandum M-24-15 on Modernizing FedRAMP section VII (a) (17) states that GSA must *"position FedRAMP as a central point of contact to the commercial cloud sector for Government-wide communications or requests for risk management information concerning commercial cloud providers used by Federal agencies."*

Purpose

FedRAMP and agency customers must have a reliable way to directly contact senior security and public sector staff operating all FedRAMP Authorized cloud service offerings without maintaining separate accounts, login procedures, or other processes for individual cloud service providers. These requirements for a FedRAMP Security Inbox apply to all cloud service providers to ensure that this direct reliable path remains open.

Once finalized, FedRAMP will perform quarterly assessments of all FedRAMP Authorized cloud service offerings by sending test messages to the FedRAMP Security Inbox on file requesting a simple human response. Cloud service offerings that fail to meet these requirements (during quarterly tests or other communications) will be **immediately suspended from the FedRAMP Marketplace for a minimum of 30 days and publicly placed on a Corrective Action Plan.**

To recover from this Corrective Action Plan and return to full service on the FedRAMP Marketplace, the providers for affected cloud services will need to demonstrate they have resolved the gap in meeting these requirements. Cloud

service offerings that are unable to address such a Corrective Action Plan within 30 days may lose their FedRAMP authorization entirely.

Expected Outcomes

- Cloud service providers will prioritize review and response of emergency time-sensitive messages from FedRAMP or other agency customers.
- Federal agencies will have a reliable way to contact security teams at cloud service providers.

Definitions

FRD-FSI-01

> **FedRAMP Security Inbox (FSI):** An email address that meets the requirements outlined in the FedRAMP Security Inbox requirements.

Requirements

FRR-FSI

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-FSI-01

> Providers MUST establish and maintain an email address to receive email regarding urgent security notifications from *all necessary parties*; this inbox is a *FedRAMP Security Inbox (FSI)*. The *FedRAMP Security Inbox* is listed in the FedRAMP Marketplace as the “Security E-mail.”

FRR-FSI-02

Providers MUST persistently ensure their *FedRAMP Security Inbox* receives email messages from .gov and .mil emails without any disruption, including meeting ALL of the following requirements when receiving an email originating from a .gov or .mil email address:

1. Messages MUST be routed to at least one senior security official who has authority to respond on behalf of the organization
2. Messages MUST NOT require manual verification from the sender, logins to a web-based system, or any other sort of authentication by the sender
3. Messages MUST NOT be automatically resolved, closed, rejected, or otherwise addressed without human review

FRR-FSI-03

Providers MUST follow the requirements and recommendations outlined in FRR-FSI-TF regarding timeframes for acknowledging and addressing messages received in their *FedRAMP Security Inbox.*

FRR-FSI-04

Providers MUST immediately notify FedRAMP of any changes in addressing for their *FedRAMP Security Inbox* by emailing info@fedramp.gov with the name and FedRAMP ID of the cloud service offering and the updated email address.

FRR-FSI-TF

This section provides guidance on timeframes that apply to all impact levels of FedRAMP authorization for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-FSI-TF-01

Providers SHOULD immediately and automatically acknowledge the receipt of messages received from *all necessary parties* in their *FedRAMP Security Inbox*.

FRR-FSI-TF-LO

This section provides guidance on timeframes that apply specifically to FedRAMP Low authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-FSI-TF-LO-01

Providers MUST have a human acknowledge and address messages sent by FedRAMP (including any @fedramp.gov address) to their *FedRAMP Security Inbox* within 3 business days.

FRR-FSI-TF-LO-02

Providers MUST have a human acknowledge and address messages sent by *all necessary parties* (other than FedRAMP) to their *FedRAMP Security Inbox* within 5 business days.

FRR-FSI-TF-MO

This section provides guidance on timeframes that apply specifically to FedRAMP Moderate authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-FSI-TF-MO-01

Providers MUST have a human acknowledge and address messages sent by FedRAMP (including any @fedramp.gov email address) to their *FedRAMP Security Inbox* within 1 business day.

FRR-FSI-TF-MO-02

Providers MUST have a human acknowledge and address messages sent by *all necessary parties* (other than FedRAMP) to their *FedRAMP Security Inbox* within 3 business days.

FRR-FSI-TF-HI

This section provides guidance on timeframes that apply specifically to FedRAMP High authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-FSI-TF-HI-01

Providers MUST have a human acknowledge and address messages sent by FedRAMP (including any @fedramp.gov email address) to their *FedRAMP Security Inbox* within 12 hours.

FRR-FSI-TF-HI-02

Providers MUST have a human acknowledge and address messages sent by *all necessary parties* (other than FedRAMP) to their *FedRAMP Security Inbox* within 1 business day.